



# UNITED STATES PATENT AND TRADEMARK OFFICE

A

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/768,154	01/24/2001	Takashi Ikeda	Q62762	3618

7590

11/15/2005

SUGHRUE, MION, ZINN, MACPEAK & SEAS  
2100 Pennsylvania Ave, N.W.  
Washington, DC 20037-3202

EXAMINER
----------

NALVEN, ANDREW L

ART UNIT	PAPER NUMBER
----------	--------------

2134

DATE MAILED: 11/15/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

<b>Office Action Summary</b>	<b>Application No.</b> 09/768,154	<b>Applicant(s)</b> IKEDA, TAKASHI	
	<b>Examiner</b> Andrew L. Nalven	<b>Art Unit</b> 2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

#### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

- 1) ☒ Responsive to communication(s) filed on 05 March 2005.
- 2a) ☒ This action is **FINAL**.                      2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

- 4) ☒ Claim(s) 1-11 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-11 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 21 March 2001 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All    b) ☐ Some \* c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)  | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)                                   | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152)             |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)<br>Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____  |

## DETAILED ACTION

1. Claims 1-11 are pending.

### ***Response to Arguments***

2. Applicant's arguments with respect to claims 1-11 have been considered but are not persuasive.
3. Applicant has argued on pages 6-7 that the Jones reference fails to teach that there is any correspondence between a second key (Jones, private key value 430) and a first key (Jones, public key value 435). Examiner respectfully disagrees. There is a direct correspondence between a public key and a private key. They work as a pair in that one key encrypts data and the other key decrypts the encrypted data. Examiner has provided a definition of public key cryptography that clearly shows the direct correspondence by stating, "the public key encrypts data, and a *corresponding* secret key decrypts."
4. Applicant has argued on page 7 that the private keys of both Schumacher and Jones fail to specify exclusively a predestinated information encryption device. Examiner respectfully disagrees. Schumacher teaches a digital camera that has associated with it a unique private key not known outside of the camera (Schumacher, column 4 lines 47-57). Since the private key is unique to the digital camera, it exclusively designates the encryption device (digital camera).

5. Applicant has argued on page 7 that the motivation to combine Schumacher and Jones is flawed because it does not address the needs of Schumacher's digital camera imaging authentication device. Examiner respectfully disagrees. Jones teaches the storage of a first and second information item (public and private keys) in a secure storage area. Jones's system provides the advantages of secure storage of these keys that prevent access to the keys to anyone who is not authorized (Jones, column 2 lines 30-45). Thus, in combining the references, Jones would offer Schumacher the advantage of secure storage of its keys. Secure storage of keys is a need of Schumacher's device because without it, Schumacher's authentication system may be compromised. Thus, Jones does provide ample motivation for the combination with the Schumacher reference.

***Claim Rejections - 35 USC § 103***

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

7. Claim 1, 4-5, 7-8, and 11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schumacher et al US Patent No 6,269,446 in view of Jones et al US Patent No 5,623,637.

8. With regards to claims 1 and 11, Schumacher discloses a unique information storage means (Schumacher, column 4 lines 47-53, ROM) for storing a first unique information item that specifies exclusively a pre-designated information encryption device (Schumacher, column 4 lines 47-53, unique private key), an encryption means for encrypting the distributed information that has been received with the first unique information item as an encryption key (Schumacher, column 4 lines 26-48, private key encrypts hash of received picture), and a decoding means for decoding the information that has been encrypted by the encryption means with a second information item as decoding key (Schumacher, column 5 lines 36-44, decrypt with public key).

Schumacher fails to teach the second unique information item that corresponds to the first unique information item being stored on the unique information storage means.

Jones teaches the second unique information item that corresponds to the first unique information item being stored on the unique information storage means (Jones, column 8 lines 47-51, Figure 3 Items 430 and 435). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Jones's second unique information item storage method with Schumacher's recording apparatus because it offers the advantage of providing secure storage for encryption/decryption keys where access is limited to authorized individuals (Jones, column 2 lines 30-45).

9. With regards to claim 4, Schumacher as modified teaches a data storage means for storing information that has been encrypted by the encryption means (Schumacher, column 4 lines 57-60, storage section).

10. With regards to claim 5, Schumacher as modified teaches the data storage means being constituted such that the storage medium into which encrypted information is written is unexchangeable fixed in the information processor (Schumacher, column 4 lines 1-3, not removable).

11. With regards to claim 7, Schumacher as modified teaches a network interface means for taking in distributed information (Jones, Figure 1, Item 173, column 3 lines 60-62).

12. With regards to claim 8, Schumacher as modified teaches the first unique information item being stored before the information processor reaches a user (Schumacher, column 4 lines 47-56).

13. Claims 2 and 9 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schumacher et al US Patent No 6,269,446 and Jones et al US Patent No 5,623,637 as applied to claim 1 above, and further in view of Nash US Patent No. 4,555,591.

14. With regards to claim 2, Schumacher as modified above fails to teach the unique information storage means being a read-only storage medium that permits only reading of the unique information items that have been stored. Nash teaches the unique information storage means being a read-only storage medium that permits only reading of the unique information items that have been stored (Nash, column 2 lines 45-59, permanently burned and can only be read, Abstract). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Nash's method of making the storage medium read only with Schumacher as modified because

it offers the advantage of preventing the key from being altered by an attacker or read by a user outside of the encryption device (Nash, column 1 lines 7-13).

15. With regards to claim 9, Schumacher as modified fails to teach the unique information storage means is provided with a register. Nash teaches the unique information storage means is provided with a register (Nash, column 2 lines 45-49). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Nash's method of using registers for unique information storing means with Schumacher as modified because registers offer the advantage of extremely high speed data access.

16. Claim 3 is rejected under 35 U.S.C. 103(a) as being unpatentable over Schumacher et al US Patent No 6,269,446 and Jones et al US Patent No 5,623,637 as applied to claim 1 above, and further in view of Bruce Schneier's Applied Cryptography.

17. With regards to claim 3, Schumacher as modified fails to teach the encryption and decoding key being the same. Schneier teaches the encryption and decoding key being the same (Schneier, Section 1.1, Page 3 Paragraph 4, Page 4 "Symmetric Algorithms"). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Schneier's method of identical keys with Schumacher as modified because it offers the advantage of allowing the use of symmetric key algorithms that offer high efficiency and performance and strong encryption (Schneier, Page 216, Section 10.2).

18. Claims 6 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schumacher et al US Patent No 6,269,446 and Jones et al US Patent No 5,623,637 as applied to claim 4 above, and further in view of Ansell et al US Patent No 6,367,019. Ansell discloses a copy security system for portable music players.

19. With regards to claim 6, Schumacher as modified fails to teach the data storage means being constituted such that the storage medium into which encrypted information is written is interchangeably installed in the information processor. Ansell teaches the data storage means being constituted such that the storage medium into which encrypted information is written is interchangeably installed in the information processor (Ansell, column 9 lines 1-13). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Ansell's method of making storage interchangeable with Schumacher as modified because it offers the advantage of affording an owner of a digital storage unimpeded convenience of use of digital media by allowing use on a number of storages while maintaining copyright protection for the digital media (Ansell, column 1 line 66 – column 2 line 3, column 2 line 46 – column 3 line 15).

20. Claim 10 is rejected under 35 U.S.C. 103(a) as being unpatentable over Schumacher et al US Patent No 6,269,446 and Jones et al US Patent No 5,623,637 as applied to claim 8 above, and further in view of Lee US Patent No. 5,790,663.

21. With regards to claim 10, Schmacher as modified fails to teach the first unique information item being a serial number that is assigned to the information processor.



Lee teaches the first unique information item being a serial number that is assigned to the information processor (Lee, column 5 lines 1-5). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Lee's method of using serial numbers with Schumacher as modified because it offers the advantage of allowing the unique identification of a processor that can facilitate tracing of a product in the field back to an original equipment manufacturer (Lee, column 1 lines 12-22).

### ***Conclusion***

**THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the mailing date of this final action.

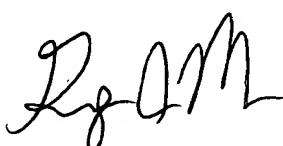
Art Unit: 2134

22. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Andrew L. Nalven whose telephone number is 571 272 3839. The examiner can normally be reached on Monday - Thursday 8-6, Alternate Fridays.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached on 571 272 3838. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Andrew Nalven



GREGORY MORSE  
SUPERVISOR, PATENT EXAMINER  
TECHNOLOGY CENTER 2100